

Practitioner's Docket No. 035-005

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of
Inventor(s):

BRIAN J. VENEKLAKE

WARNING:

Patent must be applied for in the name(s) of all of the actual inventor(s). 37 CFR 1.41(a) and 1.53(b).

For (title):

COMPUTER SECURITY SYSTEM

CERTIFICATION UNDER 37 C.F.R. 1.10*
(Express Mail label number is mandatory.)
(Express Mail certification is optional.)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date April 1, 1999, in an envelope as "Express Mail Post Office to Addressee," mailing label number EI858836425US addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature

Warning: Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

Warning: Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. 1.10(b).

"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition." Notice of October 24, 1996, 60 Fed. Reg. 56, 439, at 56, 442.

1. Type of Application

This new application is for a(n)

(check one applicable item below)

☒ Original (nonprovisional)

☐ Design

☐ Plant

WARNING: Do not use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. 371(c)(4) , unless the International Application is being filed as a divisional, continuation or continuation-in-part application.

WARNING: Do not use this transmittal for the filing of a provisional application.

NOTE: If one of the following 3 items apply, then complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED** and a **NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION**.

☐ Divisional.

☐ Continuation.

☐ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. 119(e), 120, or 121)

NOTE: If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. 120, 121 or 365(c) , the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. 120, 121 or 365(c) . (35 U.S.C. 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. 119, 365(a) or 365(b) .) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

WARNING: When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application must be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).

☐ The new application being transmitted claims the benefit of prior U.S. application(s).
Enclosed are **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

3. Papers Enclosed That Are Required for Filing Date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

Pages of specification 24

Pages of claims 2

Pages of Abstract 1

Sheets of drawing 6

☐ formal

☒ informal

WARNING: DO NOT submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. Comments on proposed new 37 CFR 1.84 . Notice of March 9, 1988 (1990 O.G. 57-62).

NOTE: "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page." 37 C.F.R. 1.84(c)).

(complete the following, if applicable)

- ☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. 1.84(b).

4. Additional papers enclosed

- ☐ Preliminary Amendment
☐ Information Disclosure Statement (37 C.F.R. 1.98)
☐ Form PTO-1449 (PTO/SB/08A and 08B)
☐ Citations
☐ Declaration of Biological Deposit
☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.
☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative
☐ Special Comments
☐ Other

5. Declaration or oath

- ☐ Enclosed
Executed by

(check all applicable boxes)

- ☐ inventor(s).
☐ legal representative of inventor(s).
37 CFR 1.42 or 1.43.
☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.
☐ This is the petition required by 37 CFR 1.47 and the statement required by 37 CFR 1.47 is also attached. See item 13 below for fee.
☒ Not Enclosed.

WARNING: Where the filing is a completion in the U.S. of an International Application, but where a declaration is not available, or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

☐ Application is made by a person authorized under 37 C.F.R. 1.41(c) on behalf of all the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 CFR 1.16(e) can be filed subsequently).

NOTE: It is important that all the correct inventor(s) are named for filing under 37 CFR 1.41(c) and 1.53(b).

☐ Showing that the filing is authorized.
(not required unless called into question. 37 CFR 1.41(d))

6. Inventorship Statement

WARNING: If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.

The inventorship for all the claims in this application are:

☒ The same.

or

☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

☐ is submitted.

☐ will be submitted.

7. Language

NOTE: An application including a signed oath or declaration may be filed in a language other than English. A verified English translation of the non-English language application and the processing fee of \$130.00 required by 37 CFR 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 CFR 1.52(d).

NOTE: A non-English oath or declaration in the form provided or approved by the PTO need not be translated. 37 CFR 1.69(b).

☒ English

☐ Non-English

☐ The attached translation is a verified translation. 37 C.F.R. 1.52(d).

8. Assignment

☐ An assignment of the invention to _____

☐ is attached. A separate "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

☒ will follow.

NOTE: "If an assignment is submitted with a new application, send two separate letters-one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).

WARNING: A newly executed "CERTIFICATE UNDER 37 CFR 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. no.	Filed
---------	------------	-------

Country	Appln. no.	Filed
---------	------------	-------

Country	Appln. no.	Filed
---------	------------	-------

from which priority is claimed

☐ is (are) attached.

☐ will follow.

NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 CFR 1.55(a) and 1.63.

NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

10. Fee Calculation (37 C.F.R. 1.16)

A. ☒ Regular application

CLAIMS AS FILED			
Number filed	Number Extra	Rate	Basic Fee 37 CFR 1.16(a) \$760.00
Total			
Claims (37 CFR 1.16(c))	6-20 = ×	\$18.00	\$0.00
Independent Claims (37 CFR 1.16(b))	5 -3 = 2 ×	\$78.00	\$156.00
Multiple dependent claim(s), if any(37 CFR 1.16(d))	+	\$270.00	\$0.00

☐ Fee for extra claims is not being paid at this time. (37 CFR 1.16(d))

☐ Amendment canceling extra claims is enclosed.

☐ Amendment deleting multiple-dependencies is enclosed.

NOTE: If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 CFR 1.16(d).

Filing Fee Calculation \$ 916.00

- B. ☐ Design application
(\$320.00--37 CFR 1.16(f))

Filing Fee Calculation \$ _____

- C. ☐ Plant application
(\$530.00--37 CFR 1.16(g))

Filing Fee Calculation \$ _____

11. Small Entity Statement(s)

- ☐ Verified Statement(s) that this is a filing by a small entity under 37 CFR 1.9 and 1.27 is (are) attached.

WARNING: *"Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. A nonprovisional application claiming benefit under 35 U.S.C. 119(e), 120, 121 or 365(c) of a prior application may rely on a verified statement filed in the prior application if the nonprovisional application includes a reference to a verified statement in the prior application or includes a copy of the verified statement filed in the prior application if status as a small entity is still proper and desired." 37 C.F.R. § 1.28(a).*

(complete the following, if applicable)

- ☐ Status as a small entity was claimed in prior application
_____/_____, filed on _____, from which benefit is
being claimed for this application under:

35 U.S.C. ☐ 119(e),
☐ 120,
☐ 121,
☐ 365©,

and which status as a small entity is still proper and desired.

- ☐ A copy of the verified statement in the prior application is included.
Filing Fee Calculation (50% of A, B or C above)

\$ 458.00

NOTE: *Any excess of the full fee paid will be refunded if a verified statement and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 CFR 1.28(a).*

12. Request for International-Type Search (37 C.F.R. 1.104(d))
(complete, if applicable)

- ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

☒ Not Enclosed

☒ No filing fee is to be paid at this time.

(This and the surcharge required by 37 C.F.R. 1.16(e) can be paid subsequently.)

☐ Enclosed

☐ Basic filing fee \$ 458.00

☐ Recording assignment

(\$40.00; 37 C.F.R. 1.21(h))

(See attached "COVER SHEET FOR
ASSIGNMENT ACCOMPANYING NEW
APPLICATION".)

\$ _____

☐ Petition fee for filing by other than all the
inventors or person on behalf of the inventor

where inventor refused to sign or cannot be
reached (\$130.00; 37 C.F.R. 1.47 and 1.17(h))

\$ _____

☐ For processing an application with a
specification in a non-English language
(\$130.00; 37 C.F.R. 1.52(d) and 1.17(h))

\$ _____

☐ Processing and retention fee
(\$130.00; 37 C.F.R. 1.53(d) and 1.21(l))

\$ _____

☐ Fee for international-type search report
(\$40.00; 37 C.F.R. 1.21(e))

\$ _____

NOTE: 37 CFR 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 CFR 1.53(d) and this, as well as the changes to 37 CFR 1.53 and 1.78 , indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from notification under § 53(d).

Total fees enclosed \$ 0.00

14. Method of Payment of Fees

☒ Check in the amount of \$ 0.00

☐ Charge Account No. 03-1723 in the amount of \$ _____

A duplicate of this transmittal is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 CFR 1.22(b) .

15. Authorization to Charge Additional Fees

WARNING: *If no fees are to be paid on filing, the following items should not be completed.*

WARNING: *Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.*

☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 03-1723

☒ 37 C.F.R. 1.16(a), (f) or (g) (filing fees)

☒ 37 C.F.R. 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: *Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 CFR 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.*

☒ 37 C.F.R. 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

☒ 37 C.F.R. 1.17 (application processing fees)

WARNING: *While 37 CFR 1.17(a), (b), (c) and (d) deal with extensions of time under § 1.136(a), this authorization should be made only with the knowledge that: "Submission of the appropriate extension fee under 37 C.F.R. 1.136(a) is to no avail unless a request or petition for extension is filed." (Emphasis added). Notice of November 5, 1985 (1060 O.G. 27).*

☐ 37 C.F.R. 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. 1.311(b))

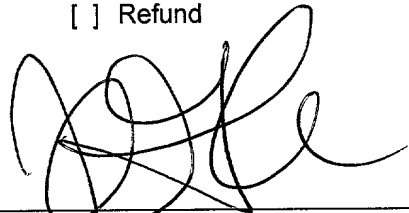
NOTE: *Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 CFR 1.311(b).*

NOTE: *37 CFR 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application ... prior to paying, or at the time of paying, ... issue fee." From the wording of 37 CFR 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.*

16. Instructions as to Overpayment

☒ Credit Account No. 03-1723

☐ Refund



John G. Chupa (Reg. No. 33,483)

Date

Chupa & Alberti, P.C.

31313 Northwestern Highway

Suite 205

Farmington Hills, MI 48334

(248) 865-9588

4/1/99

[illegible]

☐ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added _____

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

(Application Transmittal [4-1] – page 9 of 9)

**SECURE COMMUNICATIONS
METHODOLOGY AND COMPUTER SYSTEM
UTILIZING THE METHODOLOGY**

INVENTOR:
Brian J. Veneklas

SECURE COMMUNICATIONS METHODOLOGY AND COMPUTER SYSTEM UTILIZING THE METHODOLOGY

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

This invention generally relates to a secure communications methodology and to a computer system using such a methodology, and more particularly to a computer system having improved communications and security features, the communications and security features being adapted for use in a wide variety of applications and computer systems and being further adapted to allow for relatively secure and selective computer, data, and other types of information communication to occur.

2. BACKGROUND

Computer systems have become an essential tool in most of today's business activities. Importantly and by way of example, these computer systems have become critical to the on-going overall operation of many important industries, such as and without limitation, the banking, finance, travel, and commodities trading industries. It has been widely noted that while these computer systems have become quite sophisticated they have remained and/or have become concomitantly quite susceptible to unwanted and undesired "break-ins", data and communication "capture", and security "failures" resulting in an undesirable disruption to the various businesses in which they are employed and resulting in a loss and/or an undesired modification/extraction of sensitive data. In fact, many industry observers have consistently noted that undesired interception

of data communications is a very serious problem facing each and every business utilizing any form of networked computer and/or networked communications.

To address these problems and security threats many types of communications systems and methods have been developed in an attempt to reduce the number of unauthorized individuals obtaining access to the "target" system (e.g. the desired recipient of the generated communication information) and/or to somehow intentionally alter and/or modify the content of the transmitted message in a manner in which the message and/or data is "scrambled" or made allegedly "indecipherable" to someone not having the knowledge of the manner in which the received data is to be deciphered or "descrambled". In this manner, these prior systems and methodologies attempted to make it difficult for the unauthorized recipient of the message to understand and/or comprehend the meaning or actual information content contained within the communicated message.

While somewhat effective, many of these prior systems and prior methodologies have failed to adequately and desirably protect the "target" computer system against unwanted and undesired intrusion and have failed to adequately "mask" and/or "protect" the transmitted and generated data in a manner which adequately and desirably protects the data against unwanted "extraction", "descrambling" and "decoding". In sum, none of these prior computer systems and/or security and/or communications methodologies have adequately provided a desired level of security protection necessary to adequately and desirably ensure against unwanted system intrusion/modification and/or against unwanted and undesired communications interception, thereby substantially guarding against undesired system disruption and/or undesired data reception.

There is therefore a need for an improved computer security system and/or a computer and/or communications system methodology which increases the overall probability for secure communications and for secure system processing and operation while concomitantly reducing the overall probability of undesired and unwanted data extraction. Applicant's invention addresses these needs and overcomes the various drawbacks of these prior communications and computer systems.

SUMMARY OF THE INVENTION

It is a first object of the invention to provide a computer and/or communications system and/or methodology which overcomes some or all of the drawbacks of the prior art.

It is a second object of the invention to provide a networked computer system having enhanced security features and which overcomes some or all of the drawbacks of the prior art systems.

It is a third object of the invention to provide a communications methodology which allows for the relatively secure transmission and reception of data and which overcomes at least some of the drawbacks of the prior art.

It is a fourth object of the invention to provide a communications methodology which overcomes some or all of the various drawbacks of the prior art and which further allows for the selective and relatively secure communication of data, and which is further adapted for selective use on or in combination with a wide variety of computer and communication systems, including those conventional and commercially available systems used by a wide variety of businesses and other organizations.

It is a fifth object of the present invention to provide a computer and/or communications system which overcomes some or all of the various disadvantages of the prior art and which further includes a method to cause the communicated data to identify only memory locations within the central processor assembly of the "target" computer system. According to this fifth aspect of the present invention, the identified memory locations selectively house and/or store predetermined commands which, once addressed by the communicated data and/or by the central processor of the target computer system in response to the receipt of the communicated data, causes the central processor and/or other components of the processor assembly to perform one or more predetermined and desired functions and/or actions in a desired sequence of operations and/or time.

It is a sixth object of the present invention to provide a communications methodology which provides for the use of a plurality of filters which cooperate to alter and/or modify received data according to a predetermined and/or desired methodology and thereafter to transmit the modified data and/or information, thereby resulting in the communication of relatively secured data transmissions to one or more target computer systems.

It is a seventh object of the present invention to provide a data communications system and methodology which provides for the receipt of certain data and which further provides for the selective parsing and independent transmission of the parsed data according to a desired algorithm, and the utilization of a plurality of data paths and/or channels, thereby making it relatively difficult to reconstitute the entire generated data stream and increasing the overall probability that the entire transmitted data stream will not be undesirably captured.

According to a first aspect of the present invention a data or “selection/recognition” grid is provided which selectively defines those elements and/or portions of a received set of data (e.g. a “signaling” or “initiating” computer system) which comprise a message to be communicated by the sender of the set of data to the recipient and/or “target” computer system. The “recognition” grid may constitute an algorithm or a physical and portable template which may be selectively placed upon a computer screen monitor and which may be used to define those portions of the screen from which data/information is to be read or extracted from.

According to a second aspect of the present invention a communications methodology is provided which requires the receipt and/or generation of a data stream and the subsequent multiplexing of the received and/or generated data into a plurality of separate data channels. In one embodiment of the invention, each of the channels is adapted to be transmitted over and/or by the use of separate and/or independent communications mediums. The communications methodology of this second aspect of the present invention also requires and/or provides for the subsequent receipt of transmitted data respectively flowing through the plurality of data communication channels and/or separate mediums and the subsequent reconstitution of the received data into relatively about the same order and/or sequence that it was originally generated and/or received within. The reconstituted data may then be processed by the “target” computer system

According to a third aspect of the present invention a communications methodology is provided which requires and/or provides that data which is generated by a signaling computer and/or signaling computer system to refer to and/or point to

locations within a computer processor contained and operable within a “target” computer system. In this manner, unauthorized and/or undesired receipt of the generated data does not provide for and/or comprise actual receipt of the commands and/or data which, according to this aspect of the present invention, is stored in the memory sites and/or locations of the “target” computer system.

According to a fourth aspect of the present invention a communications methodology is provided which provides for a plurality of filters which are each adapted to be in a communications relationship and which are each adapted to alter and/or modify received data in a certain predetermined manner and to later transmit and/or communicate this altered information to another filter and/or to a “target” computer.

According to a fifth aspect of the present invention a computer system is provided which includes at least one of the communications methodologies which have been previously delineated and which comprise and/or form the aforescribed first, second, third, and/or fourth aspects of the preferred embodiment of the invention. Accordingly, as should be apparent to one of ordinary skill in the art, each of the foregoing communications methodologies may and are specifically and selectively adapted and designed to be selectively used in combination with one or more conventional and/or commercially available computer systems and are not intended to be limited to use with a particular type of computer system. Moreover, each of the previously delineated aspects of the present invention may be utilized in selective combination, thereby further increasing the overall security of the computer system.

Further objects, features, and advantages of the present invention will become apparent from a consideration of the following description and the appended claims when taken in conjunction with the accompanying drawings.

Brief Description of the Drawings

The drawings which are included within this Application for Patent are intended to aid in the understanding of the various preferred embodiments of the invention and are not intended, nor shall they be construed, as limiting the scope of the claimed inventions in any manner whatsoever. Accordingly, the attached drawings generally refer to and/or depict the following:

Figure 1 is a block diagram illustrating a plurality of computer systems which are in a selective communication and/or informational transfer relationship and which are adapted to incorporate one or more of the communications methodologies and/or aspects associated with and/or forming the various embodiments of this invention;

Figure 2 is a block diagram illustrating the use of a recognition grid to select and/or to define a portion of received data, according to one embodiment of the present invention;

Figure 3 is a block diagram of two of the computer systems shown in Figure 1 communicating in a manner illustrative of a second embodiment of this invention;

Figure 4 is a block diagram of two of the computer systems shown in Figure 1 communicating in a manner illustrative of a third embodiment of this invention; and

Figure 5 is a block diagram illustrative of a fourth embodiment of the invention;

Figure 6 is a perspective view of a fifth embodiment of the invention;

Figure 7 is a block diagram of the input/output driver shown in Figure 1;

Figure 8 is a block diagram of a filter made in accordance with an alternate embodiment of the invention;

Figure 9 is a block diagram of a computer system made in accordance with an alternate embodiment of the invention; and

Figure 10 is a block diagram of a computer system made in accordance with an alternate embodiment of the invention.

Detailed Description of the Preferred Embodiment of the Invention

Referring now to Figure 1 there is shown a computer networking communications/ information transfer system 10 having, in one embodiment, a plurality of conventional and commercially available computers 12, 14 and 16 which, in one embodiment of the invention, are each substantially identical and in a selective communications and/or informational transfer and/or informational “sharing” relationship. By way of example and without limitation, computer systems 12, 14 and 16 each comprise a commercially available Aptiva® system produced by the IBM Corporation of Armonk, New York. Alternatively, these computer systems comprise a conventional and commercially available Model 2256 Presario® System manufactured by Compaq Computer or virtually any other conventional and commercially available computer system. It should be noted that while various components are pictured and explained with respect to computer system 10, these components are equally applicable and/or found within computer systems 14 and 16. These computer components are described below, as are the various communications methodologies of the invention.

In one embodiment of the invention, each of the computer systems 12, 14 and 16 includes a processor 18, such as a commercially available Pentium® processor manufactured by the Intel Corporation of Corvallis, Oregon which operates under stored program control. Further, in one embodiment of the invention, each of these computer systems 12, 14 and 16 further includes at least one commercially available and conventional memory 19 which is communicatively and electronically coupled to the processor 18 by means of bus 15 and a conventional and commercially available input/output driver device 20. In one embodiment of the invention, driver device 20 comprises, as is best shown in Figure 7, an amplifier 202 which is physically and electrically coupled to processor 18 through bus 22 and which is further physically and electrically coupled to demodulator 203 and to modulator 204 by respective busses 206, 208. Modulator 204 is physically and electrically coupled to transmitter 210 by bus 212 and demodulator 203 is physically and electrically coupled to receiver 214 by means of bus 216. Transmitter 210 and receiver 214 are physically and electrically coupled to antenna 216 by respective busses 218, 220. The processor 18, memory 19, driver 20, monitor 24, and keyboard 26 may be considered to be and/or referred to as “componentry” of the computer system 12.

In operation, data in the form of electrical/electronic and/or optical signals emanating from processor 18, memory 15, and/or from keyboard 26 is electronically and/or optically amplified by amplifier 202 and coupled to modulator 204 where it is modulated and used to construct electrically/electronic/electromagnetic/ and/or optical signals 23, 25. These signals, as shown, emanate from driver 20 by transmitter 210 and antenna 216.

In this manner, computer 12 selectively communicates and/or transfers information with computer 14, 16. Additionally, electrical/electronic/electromagnetic/and/or optical informational signals 27, 29 emanating from respective computers 14, 16 are received by antenna 216 and physically and electronically/optically coupled to receiver 214 and demodulator 203 by the use of busses 220 and 216. The demodulated signal is then amplified by amplifier 202 and the amplified demodulated signal is physically and electronically/optically coupled to processor 18 by the use of bus 220. In this manner, computer systems 14, 16 selectively communicate with computer system 10. Such signals 23, 25, 27, 29, should be apparent to those skilled in this art, usually contain information which may be undesirably intercepted by a thief and/or by a “computer hacker”.

In the foregoing manner these computer systems 12, 14 and 16 may be and are adapted to be in a selective communication and/or informational transfer and/or “sharing” relationship. Moreover, it should be apparent to those skilled in this art that the previous description of the various components and operation of computer system 12 is equally applicable and substantially similar to the componentry and operation of systems 14 and 16. Moreover, it should be further apparent to those skilled in the art that computer systems 12, 14 and 16 may each be substantially similar to those described within the text entitled “Advanced Computer Architecture”, authored by Kai Hwang, produced by McGraw-Hill having reference number ISBN-0-07-031622-8 and which is fully and completely incorporated herein by reference, word for word and paragraph for paragraph.

Further, as shown in Figure 1, each of the computer systems 12, 14 and 16 further include a monitor 24 which is electronically and communicatively coupled to processor

18 by means of bus 31 and a keyboard 26 which is communicatively and electronically coupled to processor 16 by means of bus 33. Monitor 24 and keyboard 26 allow a user of each of the computer systems 12, 14 and 16 to selectively generate signals 23, 25, 27, 29, 400, and 120 and 122, to input and receive data and information from each of the computer systems 12, 14 and 16 and to interact with these systems 12, 14 and 16. Moreover, computer systems 14 and 16 are also in a communications relationship as shown by signals 120, 122 which are respectively generated by computers 14, 16. As used throughout this Application the term "target" system refers to a computer system which is destined or "targeted" to receive a signal transmission 23, 25, 27, 29, 400, 120, 122. The term "signaling" system refers to the computer system which generates these signals and transmits these signals to the target computer system. As should be apparent to those of ordinary skill in the art, these computer systems 12, 14 and 16 are conventional and commercially available systems which are adapted to allow the selective generation and communication of data and other types of information. It is to these conventional and commercially available computer systems to which Applicant's invention is directed according to a first object of the invention. Notwithstanding this aspect of the invention, it should also be noted that Applicant's invention is also applicable to other proprietary computer systems, thereby increasing the overall utility of Applicant's invention.

Referring now to Figure 2, there is illustratively shown a portion 40 of memory 19 having a plurality of memory locations 42(a)-42(l) which are each adapted to selectively allow electronic data (e.g. numerical data or command type data) to be stored therein. This stored data may emanate from keyboard 26 (e.g. being "input" into the

memory 19 by a system user). Alternatively and/or additionally this data may be received from the other computer systems 14, 16 by means of signals 27 and 29, and/or placed there by processor 18. As shown, memory locations 42(a)-42(l) each contain respectively received data 44(a)-44(l) which is received from keyboard 26 or from the other computer system 14, 16 and is subsequently selected according to the recognition grid aspects of at least one aspect of the present invention.

Specifically, the recognition grid, in one embodiment of the invention, comprises a set of predetermined memory locations which are, for example and without limitation, stored within processor 18 and which cooperatively define those memory locations which the computer processor 18 uses to select operating commands or data from. As should be apparent to those of ordinary skill in the art, every computer processor of the other computer system 14, 16 similarly utilizes/employs this feature.

That is, according to this aspect of the present invention, each processor of each of the communicating computer systems 12, 14, 16 has a set of known and predetermined memory locations which contain operational and/or command type data used to define the manner in which the processor performs its functions and/or its operations. In essence, according to this aspect of the invention, only certain memory locations 42(a)-42(l) represent "valid" locations (e.g. those locations that contain data to be used by the processor in defining its operations) for the storage of "real" or "operational" data which is to be read and acted upon by the processor 18. Moreover, in yet another embodiment of the invention, each of the communicating computer systems 12, 14, and 16 has knowledge of the storage sites for each of the computers 12, 14, and 16 associated with the sequence of operations to be accomplished by the respective computers and has

knowledge of the sequence that the target computers use to read this data in. The signaling computer then attempts to place desired operational data in these locations according to the sequential pattern that the target computer utilizes to read the data from. For example, and without limitation, if a signaling computer desired to have a target computer read data y_1 , y_2 , y_3 , in that particular sequence, and the signaling computer knows that the target computer recognizes operational data within memory locations 42(a), 42(b), and 42(c) and reads such operational data in this sequence, the signaling computer plans “ y_1 ” with memory location 42(a); “ y_2 ” within memory location 42(b); and “ y_3 ” within memory location 42(c) of the target computer.

To understand this first aspect or embodiment of Applicant’s invention it is first necessary to understand that in one embodiment of the invention, the received data information is sequentially placed within certain memory locations of each target computer system 12, 14, 16 (e.g. beginning at the lowest numbered memory location 42(a) and sequentially continuing towards the highest numbered memory location 42(l)) according to the instant in time in which the data was received. This is, according to this embodiment, the first (in time) data portion which is received by a target computer system 12, 14, 16 is placed in the lowest numbered memory location 42(a) which is available. The last (in time) portion of the received data is also placed into the lowest **available** memory location which is used to contain the received data. Since the last, in time, data is received **after** a sequence of data has already been received, this last received portion is placed into the highest position of any of the data received in that particular data reception sequence.

For example and without limitation, according to this aspect of the present invention, the first bit of data received is placed into the lowest numbered memory location 42(a). The next data bit received is placed into the next higher numbered memory location 42(b). The process is repeated until all of the received data bits are placed within memory locations or until all memory locations are utilized. After all of the received data 44(a)-44(l) is “stuffed” within these memory locations 42(a)-42(l), certain bits of the data 44(a)-44(l) are extracted according to the recognition grid algorithm developed by and explained by Applicant.

Particularly, this recognition “grid” algorithm (e.g. representatively shown by the closed geometric figure 33) selects and/or defines those memory locations 42(a)-42(l) representing “valid” or “operational data” and the order that the data is to be read from (e.g. the order that the data is “read from” does not necessarily need to be the order used to define how and/or the manner that the data is “stuffed” within memory). By way of example and without limitation recognition grid algorithm 33 defines data 44(c), 44(e), 44(g), 44(h), 44(j), and 44(k) as the operational data to be used by processor 18. Processor 18 is then, in one embodiment, directed to read the sequence of data beginning at the lowest memory position having “valid” data (e.g. 42(c)) and continuing in sequence until reaching the highest memory position having “valid” data (e.g. 42(k)). Here, in this example and without limitation. The sequence of operational steps performed by processor 18 is defined by the data sequence 44(c), 44(e), 44(g), 44(h), 44(j), and 44(k). In another embodiment, of the invention, the operational sequence is defined by the sequence of data represented by 44(k), 44(j), 44(h), 44(g), 44(e), and 44(c) or the exact opposite or “mirror image” of the sequence employed by the target computer

system in the first example. It should be understood that in an alternate embodiment of the invention each memory location may contain multiple bits of information.

This algorithm, in one embodiment and without limitation, is present in each of the computer systems 12, 14 and 16. Moreover, in this embodiment, every communicating computer system 12, 14, and 16 has knowledge of those memory locations which any “target” computer system regards as containing or adapted to contain “real” data (e.g. those data bits selected by the respective recognition grid of the “target” computer system), has knowledge of the sequence employed by each of the communicating computer systems 12, 14, 16 to “read” data from these “valid” locations, and has further knowledge of the manner required to place certain data in these memory locations (e.g. each time slot defines a unique memory location and the process of “stuffing” memory locations begins at the lowest numbered memory locations with the first bit received and continues or progresses to the highest numbered memory location). Hence by way of example and without limitation, a transmitting or “signaling” computer system 12, 14, 16 which desires to place data within memory location 42(a), 42(d), and 42(e) of a “target” or receiving computer system 12, 14, 16 would ensure that the first, fourth, and fifth data bits of the transmitted signal contain the respective data that is desired to be placed within these locations. The remaining transmitted data bits are irrelevant to this communication methodology, according to this aspect of the invention. Moreover, if the “target” system 12, 14, 16 operated in accordance with the teachings of the first embodiment of the invention, the operational data sequence would be defined by the order of 42(a), 42(b), and 42(c).

In this manner, by way of a second example and without limitation, the “real” data or the actual operational data (shown for illustration purposes as 44(c), 44(e), 44(g), 44(h), 44(j), and 44(k)) that is desired to be communicated by and between the computers 12, 14 and 16 is “mixed” with other filler data (44(a), 44(b), 44(d), 44(f), 44(i) and 44(l)). Such “filler” data does not affect the operation of the target or receiving computer 12, 14, 16. Access to the transmitted data 44(a)-44(l) without knowledge of the recognition grid algorithm (e.g. those memory locations and associated data representing the “real” or processor operational data) would not allow an unauthorized recipient to gain knowledge of the actual communicated operational/control information and therefore provides a relatively secure communications methodology which may be used with conventional and commercially available computer systems 12, 14 and 16 as well as by proprietary computer systems. Importantly, it should be understood that any number of storage sites 42(a) -42(l) may be designated by the “grid” algorithm and the data 44(a)-44(l) may be “read” from these sites in any order and according to any method, the only requirement being that each communicating or signaling computer system 12, 14, 16 have knowledge of those respective memory locations 42(a)- 42(f) which each of the communicating target computer systems 12, 14, 16 regards as containing operational data and the respective sequence that each of the target computer systems reads the data from.

According to another embodiment of the invention, as best shown in Figure 6, the recognition grid may comprise a generally flat and transparent template 300 which is adapted to be placed upon the generally flat surface 302 of a computer monitor and/or screen 304 which is selectively adapted to display data 306. In this manner, a user of screen 304 simply and physically places the template 300 over the screen in order to

determine the data which is “valid”. The “valid” data appears underneath of the template 300. Data, such as data 340, not appearing under the template is not considered “valid” and is irrelevant. “Valid” or operational data may be ensured to be viewed at only within the boundaries of the template 300 since positional placement upon screen 302 is directly related to positional placement within the memory 40. Hence, the shape of the template 300 defines which memory locations contain operational data. Alternatively, a user could just remember the pattern and simply read those locations included within the pattern. In this manner, the use of a separate template is obviated.

In yet an alternate embodiment of the invention, the recognition grid information (e.g. the identity of “valid” memory locations and the sequence of “reading” these locations) may be transmitted by a signaling computer 12, 14, 16 to a target computer 12, 14, 16 by use of a separate channel or signal 400. In this manner, a thief or “hacker”, in order to understand the entire content of the data transmitted between the computer systems would be required to capture both the data and the recognition grid signal. Moreover, the use of a separate channel 400 allows these memory locations and/or recognition grid algorithm to be dynamically modified and/or updated.

Referring now to Figure 5, there is shown another aspect of the communications methodology of the present invention. Particularly, there is shown a portion 60 of memory 19 having a plurality of addressed memory locations 62, 63, 64, and 65 which each respectively contain command and central information and/or data 67, 69, 71 and 72. The term “command data” and/or “central information”, as used in the description of this invention embodiment, means data which defines and/or represents certain actions

which must be undertaken by the processor 18 and which is “read” or understood by the program resident within the processor 18.

According to this aspect of the present invention, the actual command data or other information desired to be presently communicated by and between each of the computer systems 12, 14 and 16 (e.g. illustrated as data 67, 69, 71 72) are resident within each of the memory locations of each of the “target” computer systems 12, 14, 16. In this embodiment, each of the computer systems 12, 14, 16 has knowledge of the contents of each memory location in each of the other computer systems 12, 14, 16 and thus needs to merely specify memory locations, according to this communications methodology, in order for the “target” computer system 12, 14, 16, to perform some action or some sequence of actions. The signaling computer 12, 14, 16 simply directs the target computer 12, 14, 16 to perform some function or operation which already resides within the target computer 12, 14, 16. In this manner, the transmitted communications signals 23, 25, 27, 29, 120 comprise and/or include data stream 80 which comprises and/or identifies only memory locations 62, 63, 64 and 65 of the target computer system 12, 14, 16. Hence, the unauthorized receipt of the communications signals 23, 25, 27, 29, 120 provides relatively little or no information concerning the actual data or information to be communicated (e.g. the actual data commands and/or actual information located within memory locations 67, 69, 71 and 72). The command information being solely resident within each of the target computer systems 12, 14, 16 is relatively inaccessible and relatively unknown to the thief or interceptor of data stream 80, thereby substantially preventing the data recipient from gaining access to the actual information of each of these systems 12, 14 and 16.

Referring now to Figure 3 there is shown yet another aspect of the present invention. Particularly, in this embodiment of the invention, a plurality of filters 90, 92, and 94 are deployed between every two of the communicating computers, such as by way of example and without limitation, between computers 12 and 14. Each filter 90, 92, 94, according to one embodiment associated with this aspect of the present invention, includes a processor (substantially similar to processor 18 and operating under stored program control), a memory portion (substantially similar to memory 19), and an input/output driver which is substantially similar to driver 20. Moreover, according to one embodiment of the present invention, the processor memory, and driver are electrically and communicatively connected in the manner shown in Figure 1.

Particularly, each filter is adapted to receive a transmitted signal 23, 25, 27, 29, 120, 122, from any of the computer systems 12, 14, 16, and to modify the signal in a certain manner (e.g. by way of example and without limitations by performing a logical “NOT” operation on each data bit included within the received signal). Once the modified signal is received by the “target” computer system (e.g. in this example computer 12) it is changed to the original transmitted signal (e.g. by again performing a logical “NOT” operation on each of the received data bits). In this manner, unauthorized receipt of the modified signal at any stage of the transmission between the first computer system 305 and the second computer system will not allow the undesired recipient to gain knowledge of the information which was desired or which was actually transmitted by and between these two computer systems. In yet another embodiment of the invention, each filter provides and/or appends at least one “flag” or additional data bit to the received data stream to another filter and/or to the target computer system. In this

manner, the target computer system has knowledge of the path that the data undertook before it arrived at the target computer system.

Referring now to Figure 4 there is shown yet another aspect of the present communications and computer system invention. As shown, according to this aspect of the present invention, each stream of incoming data is transmitted to and received by a parser 100. According to this aspect of the present invention the parser 100 includes a computer processor, substantially similar to processor 18 and acting under stored program control, and a memory portion substantially similar to memory 19 and which contains commands which direct the operation of the processor. In this embodiment of the invention, the incoming data stream (e.g. such as that produced by processor 18 and which is desired to be communicated to computer system 14) is split into a plurality of separate channels 102, 104. Importantly, according to this aspects of the present invention, each of these plurality of separate channels 102, 104 is independently sent or transmitted to a the “target” (e.g. any of the computer systems 12, 14 and/or 16) computer system where they are reconstituted. In this manner, unauthorized receipt of one or more of these channels will not allow the recipient to gain access to the whole of the transmitted information. It should be appreciated that this passer methodology may be employed with the previously discussed transmission of memory locations and/or with the recognition grid algorithm to provide even greater security.

In yet another aspect of the present invention, as shown best in Figure 8, Filter 350, which is substantially identical to filters 90, 92, and 94 is programmed to receive a plurality of data bits 352, to analyze the data bits, and to transmit a compressed data Stream 354 having the received “valid” or operational data denoted as “ x_1 ” and “ x_2 ”.

Stream 354, in this embodiment only includes a single bit “x₃” representing all of the filler data represented as “x₄” ...x_n” in Figure 8. Alternatively by way of example and without limitation Filter 350 may generate all of the filter data, “x₄” ...x_n” but compress the “real” or operation data “x₁” and “x₂” into a single bit “xZ” which the target system realizes or has a prior knowledge of. In this manner, only the target system, within processor 18, knows that xZ uniquely “maps into” or represents the data “x₁” and “x₂”. A thief intercepting the “x₂” data would not have this mapping information. In this manner, Stream 354 may compactly communicate the filler/valid information to a target computer system.

Referring now to Figure 9, there is shown yet another embodiment of the invention. As shown, computer system 500, which may be substantially similar to computer systems 12, 14, 16 is electronically, physically, and communicatively coupled to access central device 502 which, in one embodiment, comprise a processor operating under stored program control.

As shown, a request for access signal 503 to computer 500 is received by device 502 from a user 504 who must provide a user identification number 506 as part of signal 503. The device 502 then matches the identification number 506 with other stored data such as the user’s location, and a transmitted message code 510 that is received from a pseudo random number generator 511. Device 502 then places a call to user 504 and communicates the code 510 to the user 504. Device 502 then waits a predetermined period of time before the code is “echoed back” by the user. If the “echo” matches, access is allowed.

Referring now to Figure 10 there is shown a computer security system 800 for use with a computer 810 which selectively communicates with a computer user 820. As should be appreciated by those of ordinary skill in the art user 820 may comprise a human and/or a computer machine and/or plurality of computers.

As shown, system 800 further includes a computer access and/or security module 822 including a switch 824 coupled to and in operable control communication, by means of communications bus 825 with a processor assembly 826 acting under stored program control.

As shown, assembly 826 selectively allows user 820 to communicate with computer 810 by the closing of switch 824, thereby allowing full duplex and/or half duplex communication through channels 840, 842. This switch 824 is closed only after receipt of a query signal on bus and/or communications channel/medium 844 which is sent to computer 810 by assembly 826 which utilizes communications channel/medium 846. Computer 810, in one embodiment, compares the signal with memory data and if a match is found communicates a signal 829 to processor 826 by means of communications channel/medium 848. User 820 must, within a certain time period, communicate signal 829 to processor 826 by means of bus and/or communications channel/medium 831. Once signal 829 has been received by processor assembly 826, switch 824 is closed, allowing communications between user 820 and computer 810, until no more signals and/or data is present on bus/communications channel/medium 840.

In an alternate embodiment, once switch 824 is initially closed, computer 810 transmits uniquely different signals along bus 848 to processor assembly 826 at separate and distinct periods and/or intervals of time. User 820, in order to keep the switch 824

closed, must similarly communicate these very same uniquely different signals to processor 826, along bus/communications channel/medium 831, at substantially the very same time. Alternatively, each query signal on busses 844/846 and match signal 829 is “logged” or recorded and stored within processor assembly 826 in order to create and maintain a system access record. In yet another aspect of the invention, query signal on bus 844/846 must specify the type of file, the identity of the information, and/or the security level requested within computer 810. A separate record of each such request is kept for historical record keeping purposes.

It is understood that changes and modifications may be made to the above-described inventions without departing from the spirit and the scope of the various inventions. Nothing in the description or in any other portion of this Application is intended or shall be construed as to limit the nature and the scope of the Applicants’ invention.

In the Claims:

(1) A method for communicating digital information, said method comprising the steps of:

- (a) creating filler information;
- (b) transmitting said digital information in combination with said filler information;
- (c) receiving said transmitted information;
- (d) storing said transmitted information;
- (e) creating a recognition grid; and
- (f) selecting portions of said received and stored transmitted information according to said recognition grid, thereby allowing at least a portion of said transmitted digital information to be communicated.

(2) The methods of claim 1 further comprising the step of placing the filler information in a variable pattern within the digital information.

(3) A recognition grid adapted for use with an array of memory locations, each of said memory locations having a unique address associated therewith, said recognition grid comprising an array of at least one of said unique addresses of said plurality of memory locations.

(4) A communications system comprising:

- (a) a first computer adapted to selectively generate and transmit certain information;
- (b) a second computer, in communication relationship to said first computer, and containing a plurality of addressable memory locations, and further adapted to receive said certain information, and to use this information to address said contained memory locations.

- (5) A computer communications system comprising:
- a first computer adapted to generate a signal;
 - a filter in communications relationship with said first computer and adapted to modify said signal and to transmit a second signal; and
 - a second computer in communications relationship with said filter and adapted to receive said second signal and to modify said second signal in a manner effective to create said first signal to be communicated to said second computer by said first computer.
- (6) A computer communications system comprising:
- a computer adapted to generate data;
 - a passer adapted to receive said data, to split said data, and to transmit said split data over a plurality of communications mediums; and
 - a second computer connected to said plurality of communications mediums and adapted to receive said data from said passer.

ABSTRACT OF THE DISCLOSURE

A networked computer system 10 having enhanced communications security aspects.

FIGURE 1

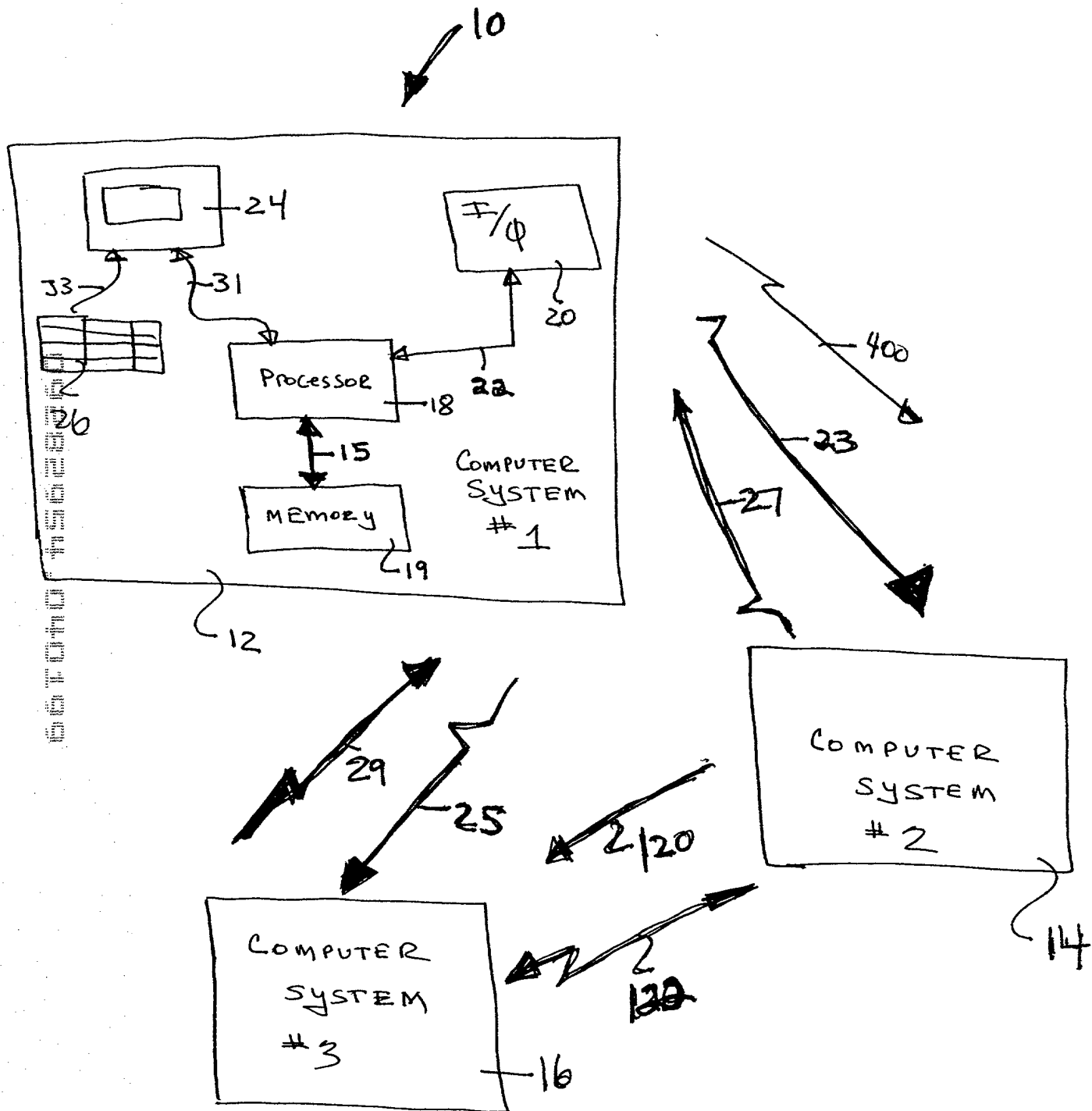


FIGURE 2

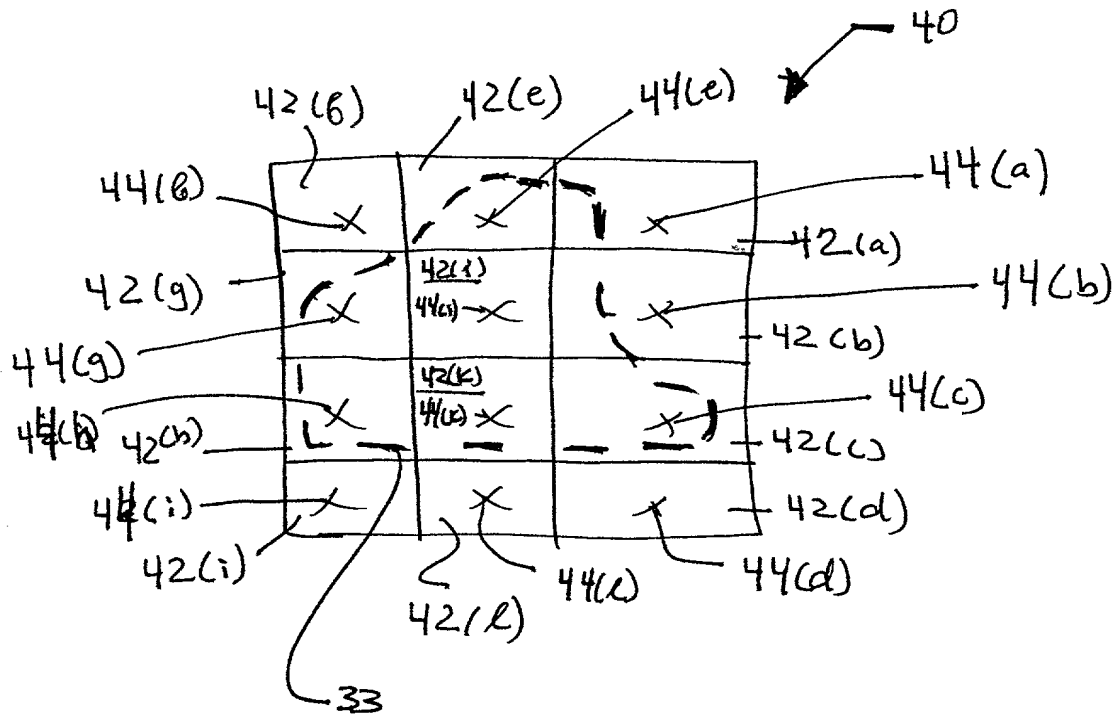


FIGURE 3

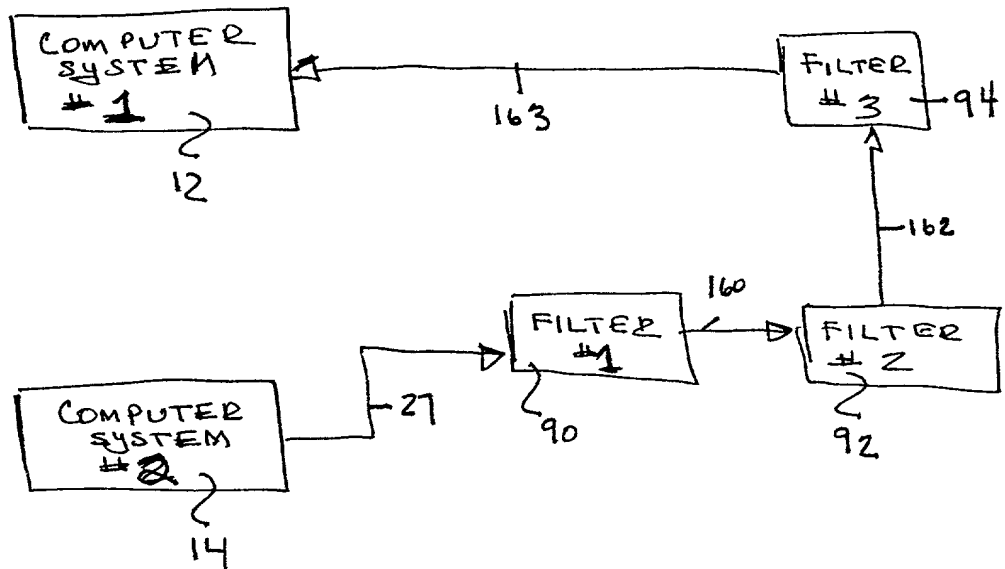


FIGURE 4

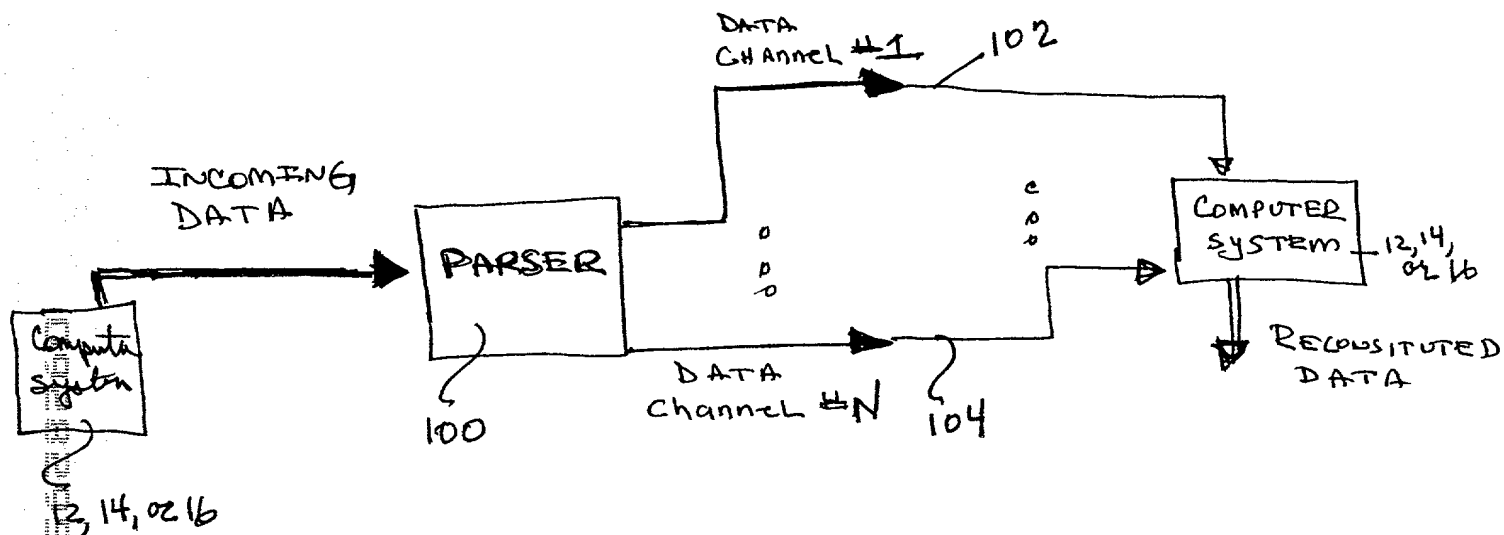


FIGURE 5

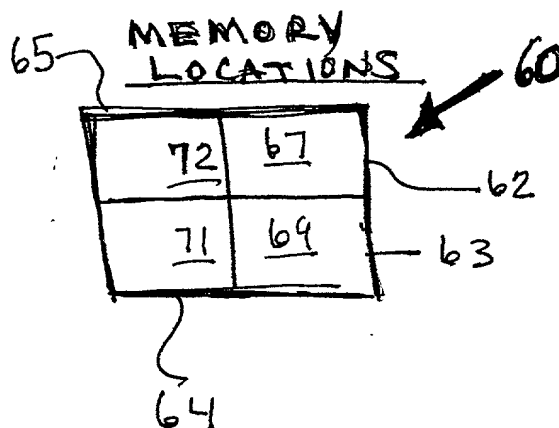
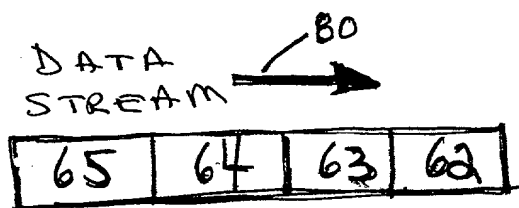


FIGURE 6

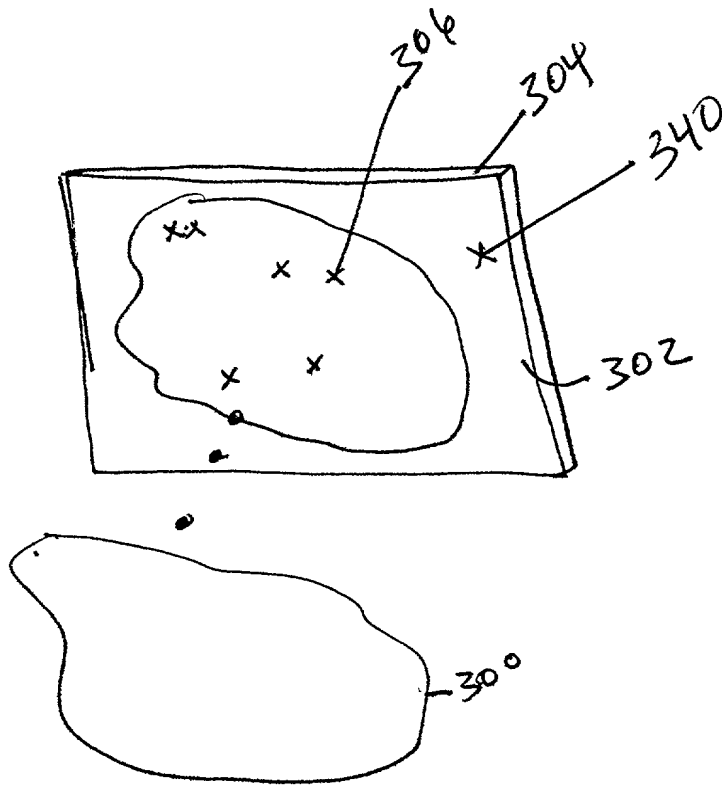


FIGURE 7

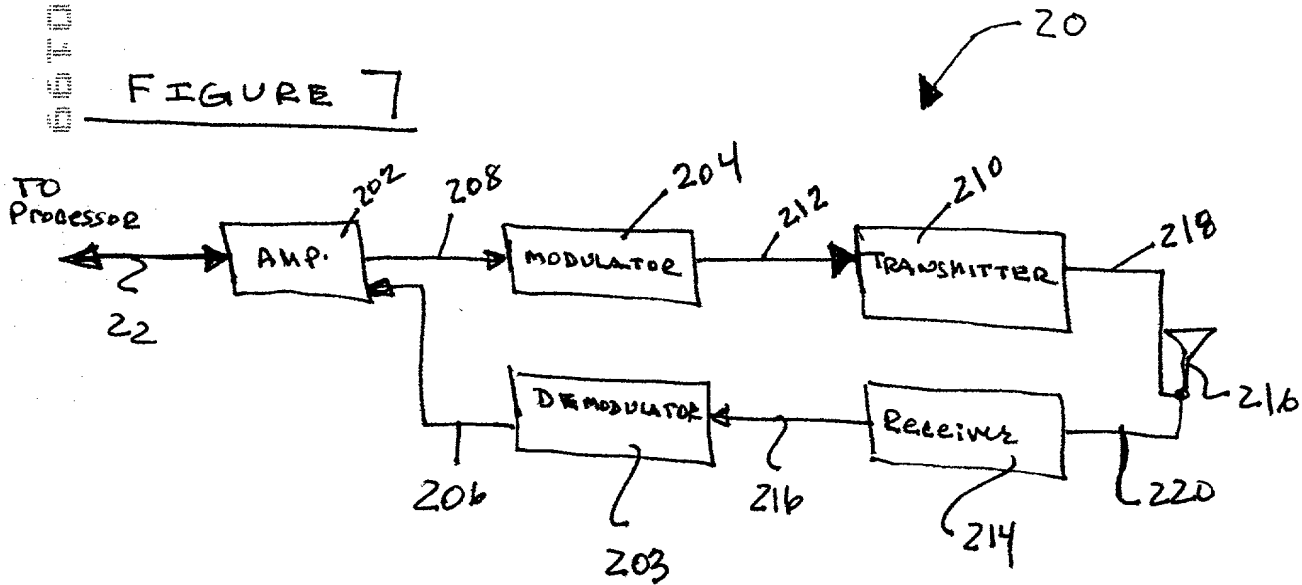


FIGURE 8

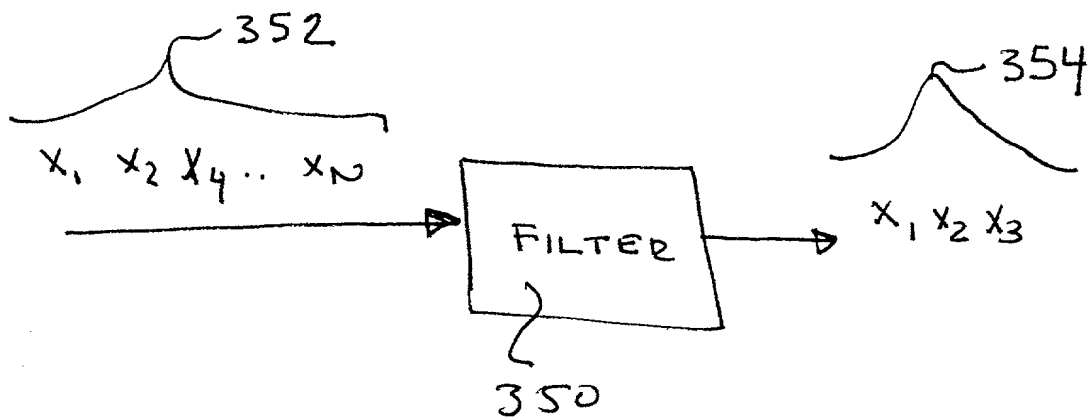


FIGURE 9

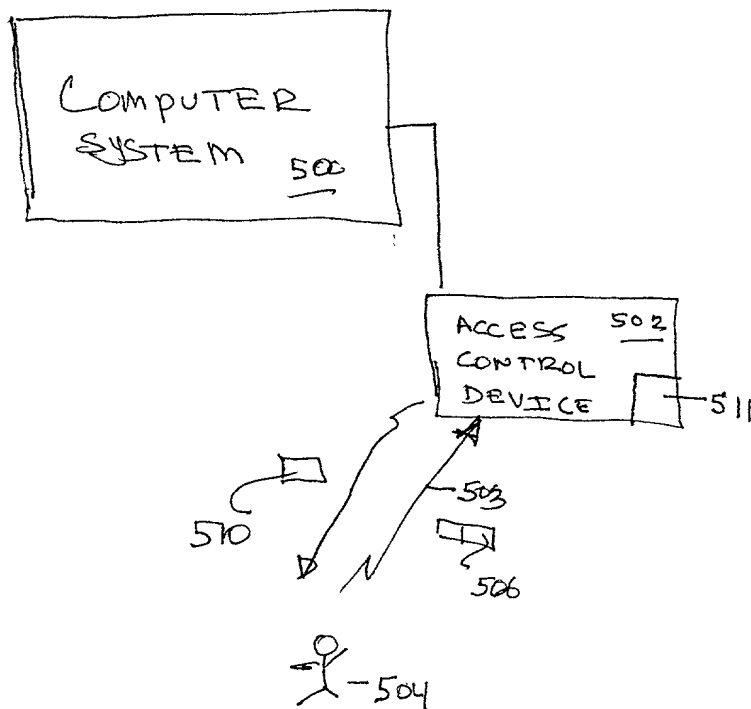


FIGURE 10

